Nota técnica

Configuración antivirus acceso Giltza

Izenpe

enero 2019

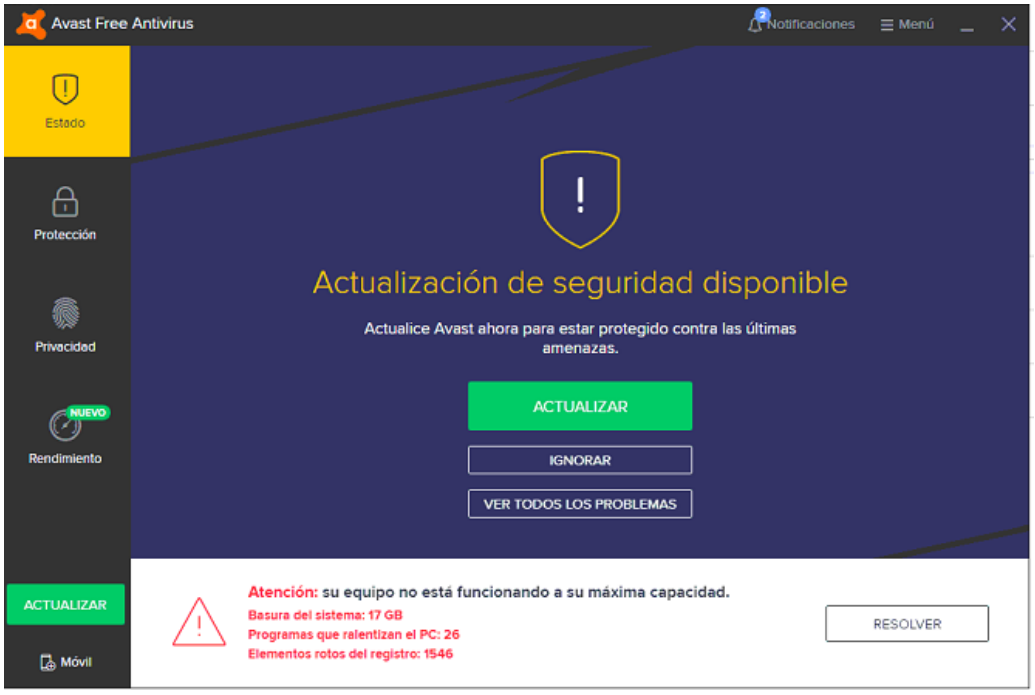
Beato Tomás de Zumárraga
71 - 1ª Planta
01008 Vitoria - Gasteiz

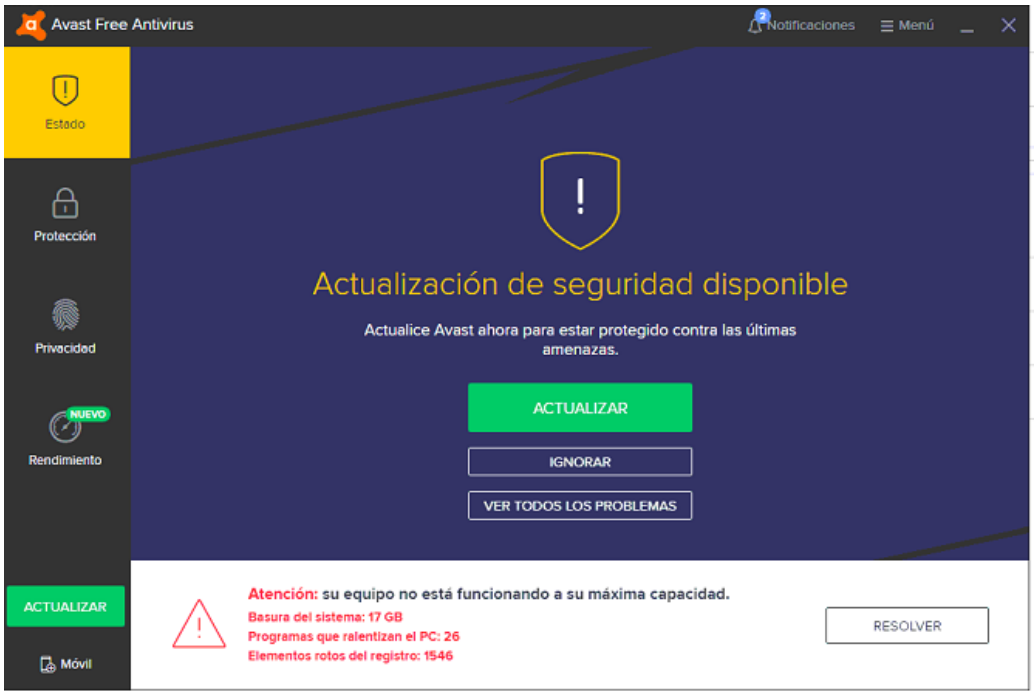
www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

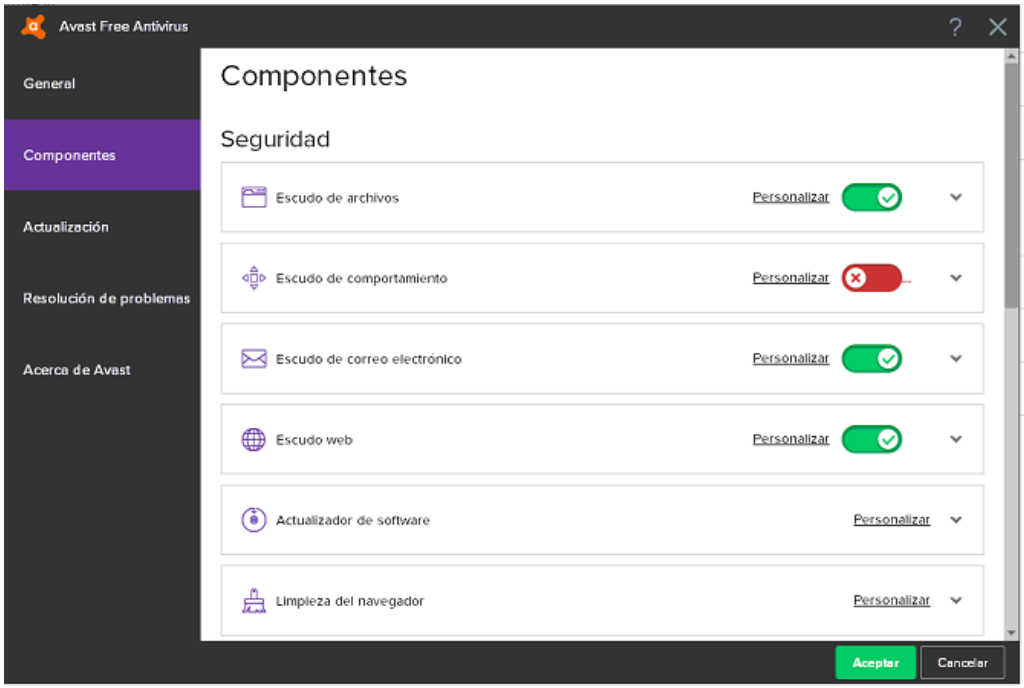
1. Configuración Antivirus Acceso GILTZA

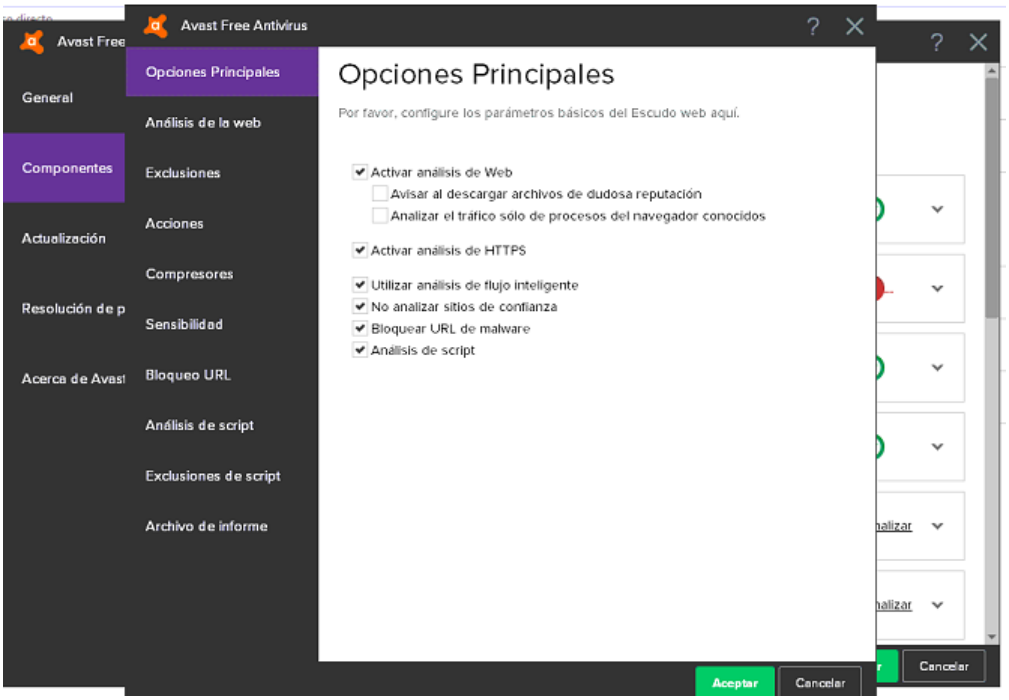
Los antivirus están incorporando una nueva protección o escudo que analiza o filtra las conexiones Seguras/Cifradas/HTTPS

1. **Avast** tiene en las opciones de escudos Web, el análisis de conexiones HTTPS. Quitando esto funciona el acceso sin problemas:

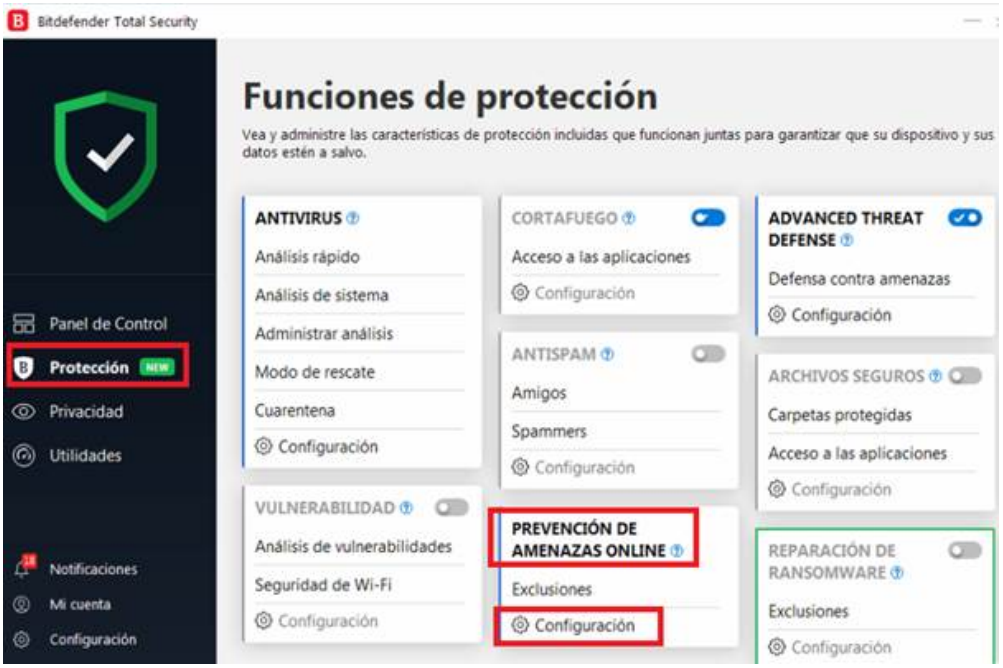




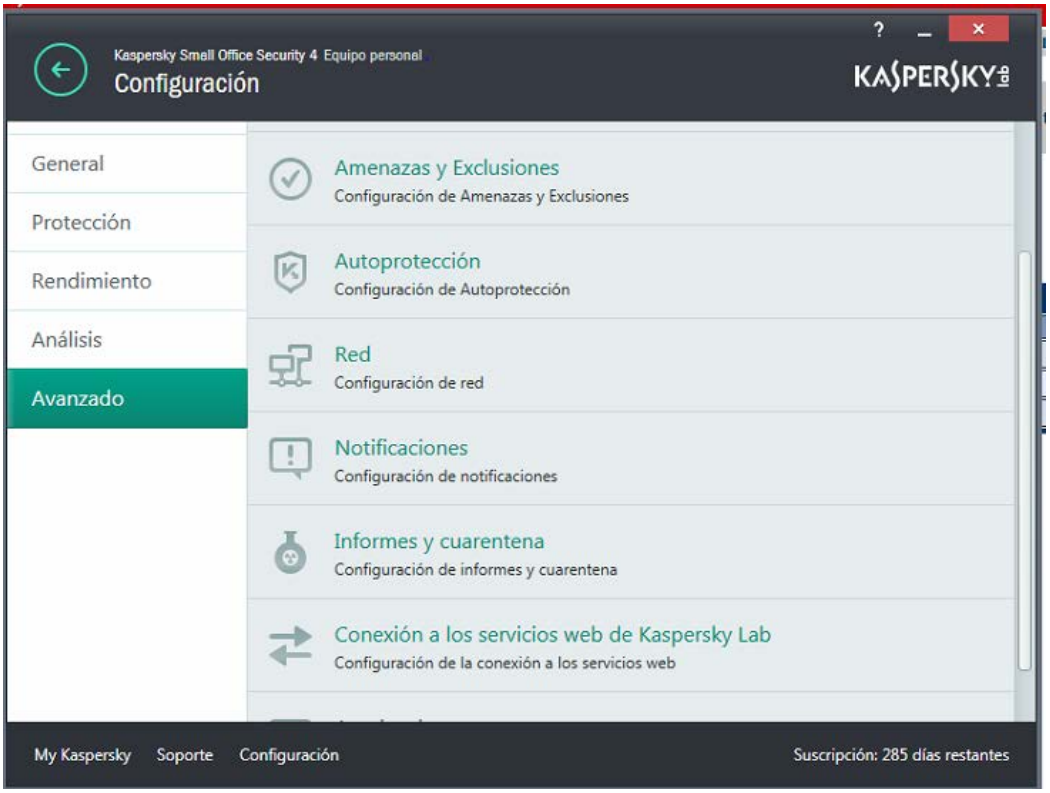

Avast Free Antivirus
General
Componentes
Actualización
Resolución de problemas
Acerca de Avast
Componentes
Seguridad
Escudo de archivos
Personalizar
Escudo de comportamiento
Personalizar
Escudo de correo electrónico
Personalizar
Escudo web
Personalizar
Actualizador de software
Personalizar
Limpieza del navegador
Personalizar
Aceptar
Cancelar

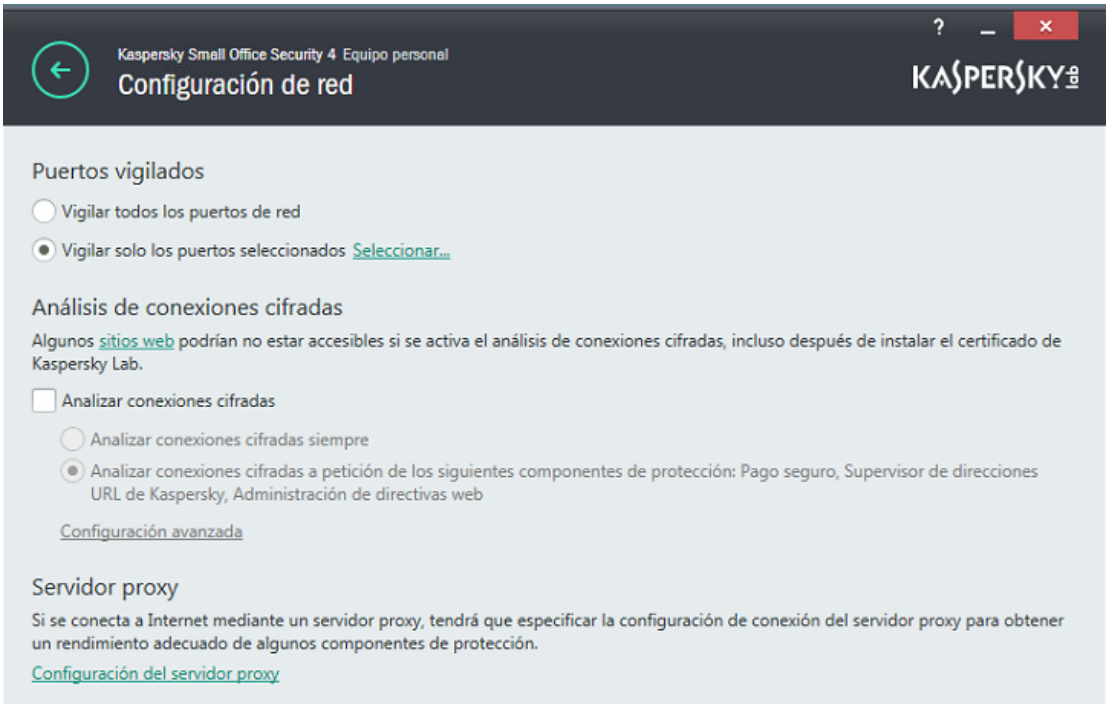

Avast Free Antivirus
Opciones Principales
Análisis de la web
Exclusiones
Acciones
Compresores
Sensibilidad
Bloqueo URL
Análisis de script
Exclusiones de script
Archivo de informe
Opciones Principales
Por favor, configure los parámetros básicos del Escudo web aquí.
Activar análisis de Web
Avisar al descargar archivos de dudosa reputación
Analizar el tráfico sólo de procesos del navegador conocidos
Activar análisis de HTTPS
Utilizar análisis de flujo inteligente
No analizar sitios de confianza
Bloquear URL de malware
Análisis de script
Aceptar
Cancelar

2. **Bitdefender** también tiene un filtro web que analiza conexiones HTTPS y evita la autenticación



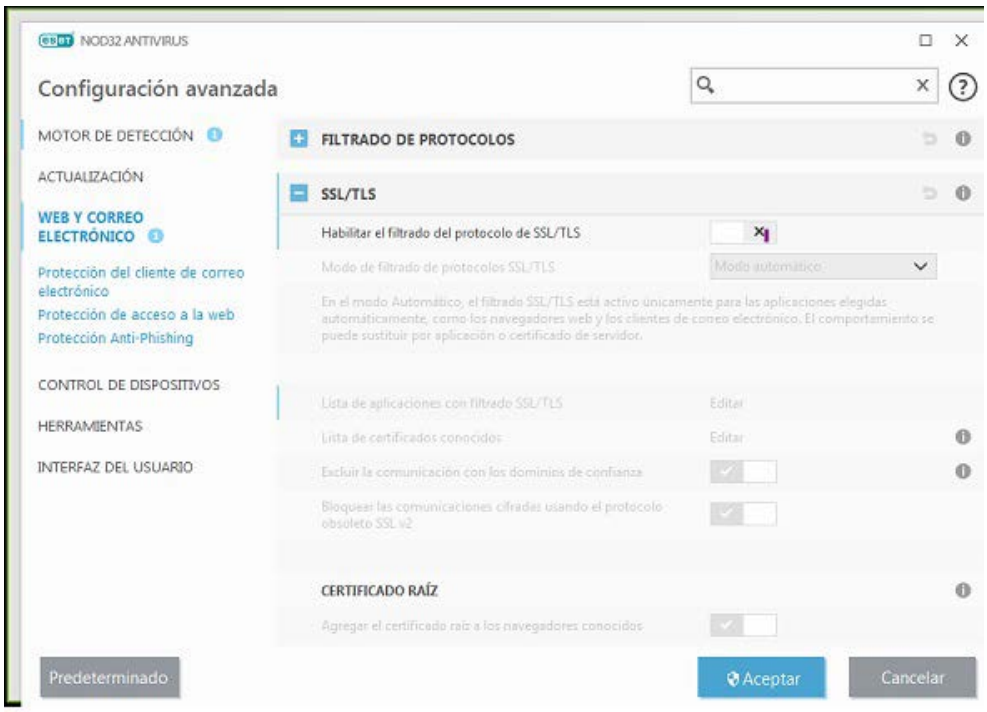
3. **Kaspersky** tiene filtros que, aunque se pausen sigue dejando de detectar los certificados (todos, tanto Izenpe como FNMT…).
   En CONFIGURACIÓN→ AVANZADO→ RED → DESMARCAR Analizar Conexiones cifradas





4. ESET NOD32

En CONFIGURACIÓN AVANZADA→ WEB Y CORREO ELECTRÓNICO→PROTECCIÓN DE ACCESO A LA WEB → DESMARCAR Habilitar el filtrado del protocolo de SSL/TLS

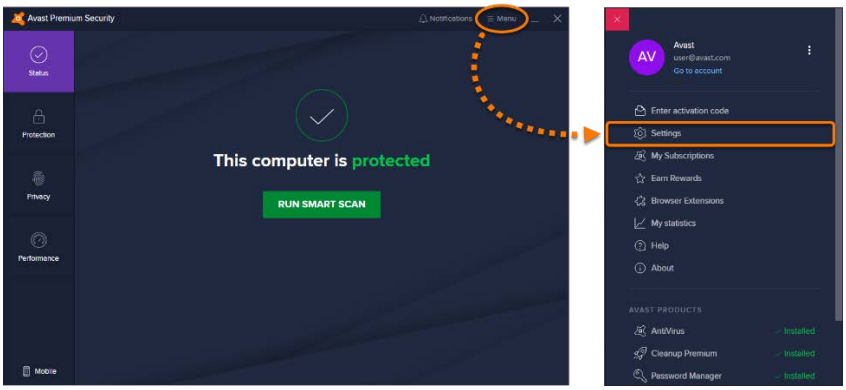


2. Configuración Antivirus – Sitios de confianza

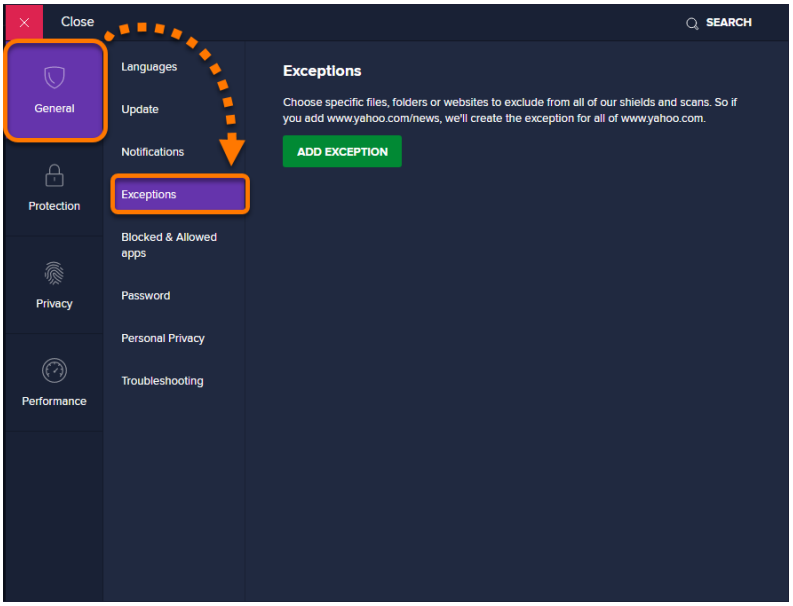
Aunque por lo general no se recomienda, puede que quiera excluir del análisis determinados archivos, carpetas o sitios web para acelerar el proceso o evitar que se detecten falsos positivos. Esto se puede hacer añadiendo archivos individuales, carpetas enteras o sitios web a la lista de excepciones. Los elementos de la lista de excepciones se excluyen de todos los análisis y escudos

1. AVAST ANTIVIRUS

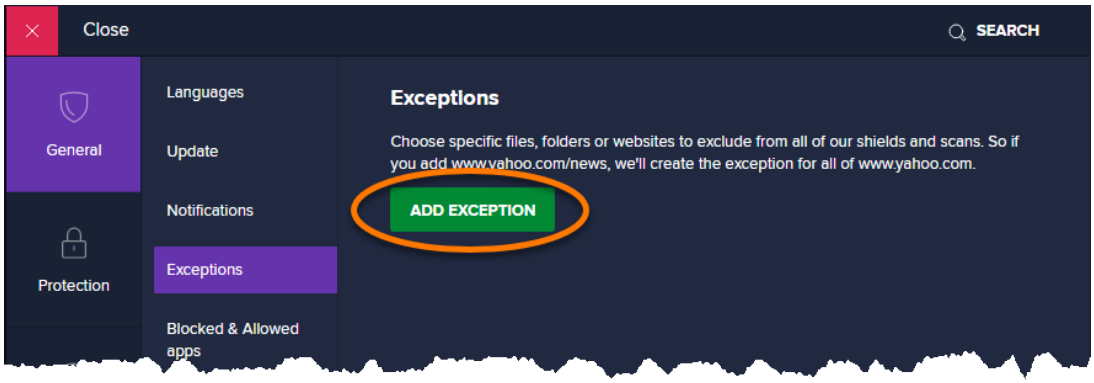
1. Abra Avast Antivirusy vaya a **Menú** ▸ **Opciones**.



2. Seleccione **General** ▸ **Excepciones**.

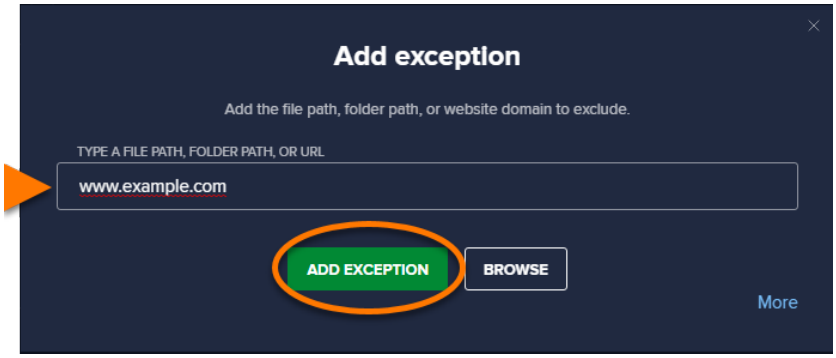


3. Haga clic en **Añadir una excepción**.

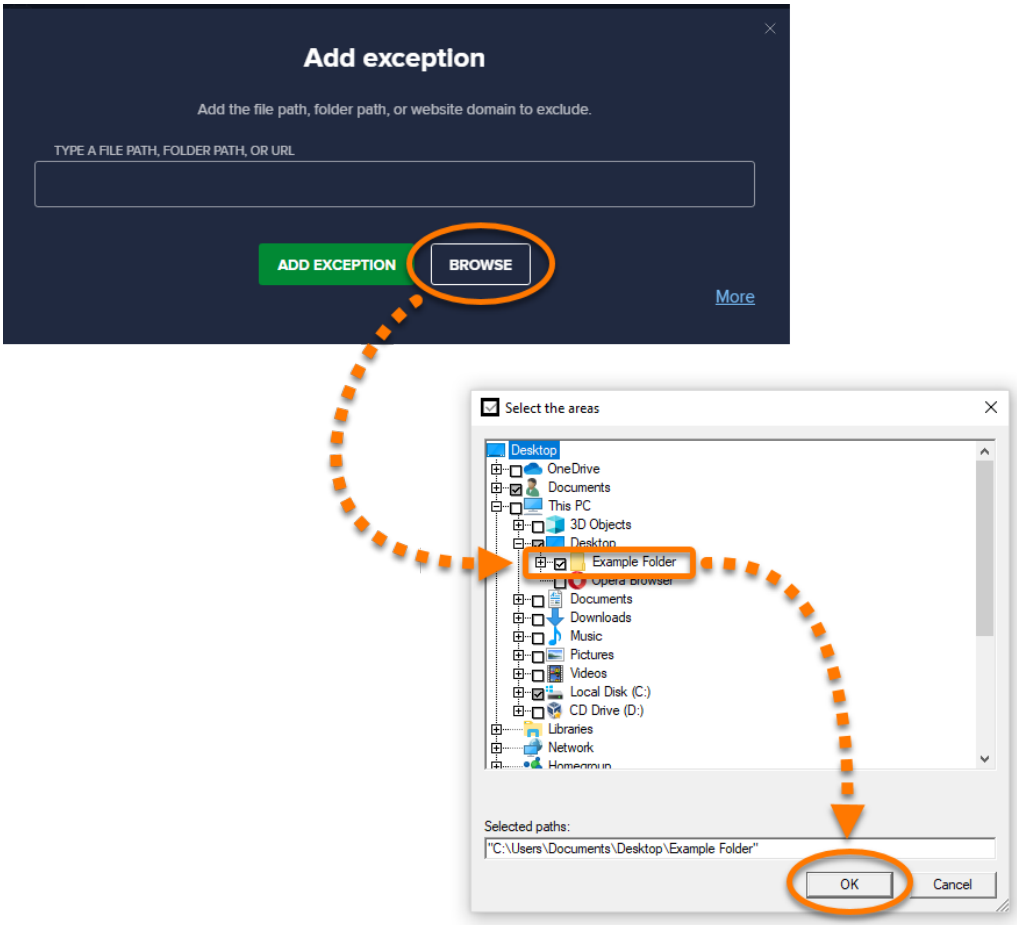


4. Las excepciones se pueden añadir de varias formas:

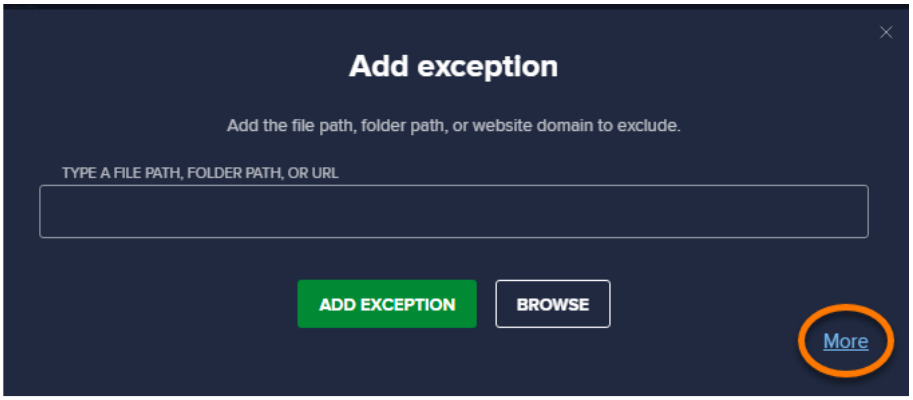
   - Escriba la ruta específica del archivo o de la carpeta, o la URL, en el cuadro de texto y, a continuación, haga clic en **Añadir una excepción**.

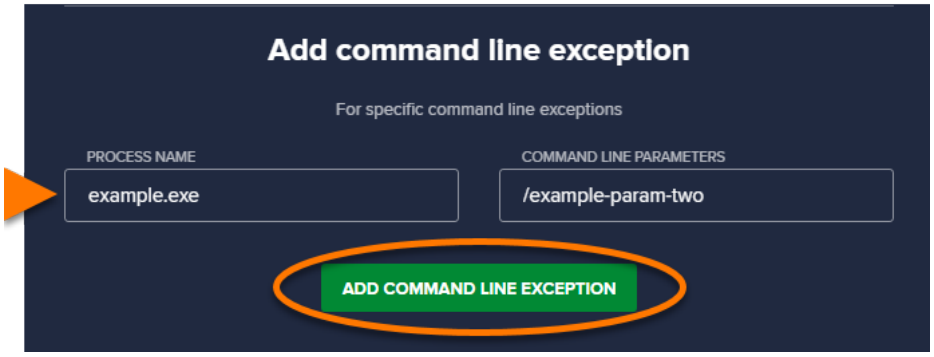


   - Haga clic en **Examinar**, marque la casilla situada junto al archivo o la carpeta que desea excluir y, a continuación, haga clic en **Aceptar**.



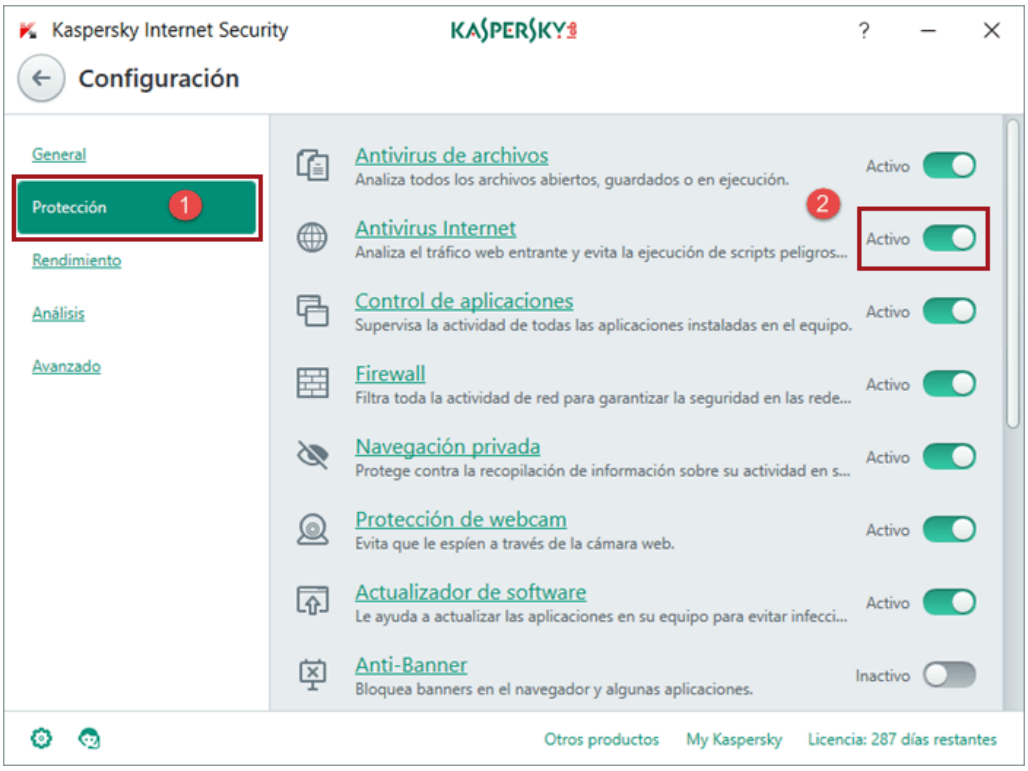
5. Haga clic en **Más**, rellene los campos **Nombre del proceso** y **Parámetros de línea de comandos** y, a continuación, haga clic en **Añadir excepción sin archivo**.



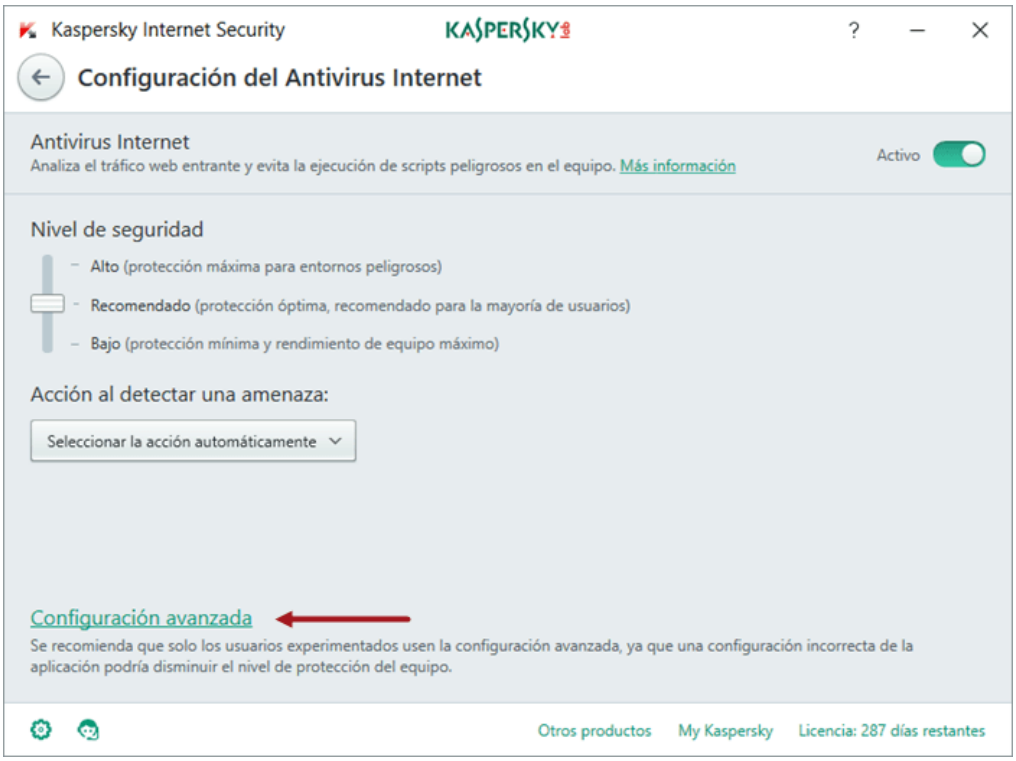


2. KASPERSKY ANTIVIRUS

1. Abre los ajustes de Kaspersky Internet Security y selecciona *Protección -> Antivirus Internet*.



2. En la ventana de configuración, selecciona *Configuración avanzada*.



3. Selecciona *En todos los* sitios *web excepto en aquellos especificados* y añade los enlaces que no quieres que compruebe Kaspersky Internet Security (dentro de Administrar exclusiones).